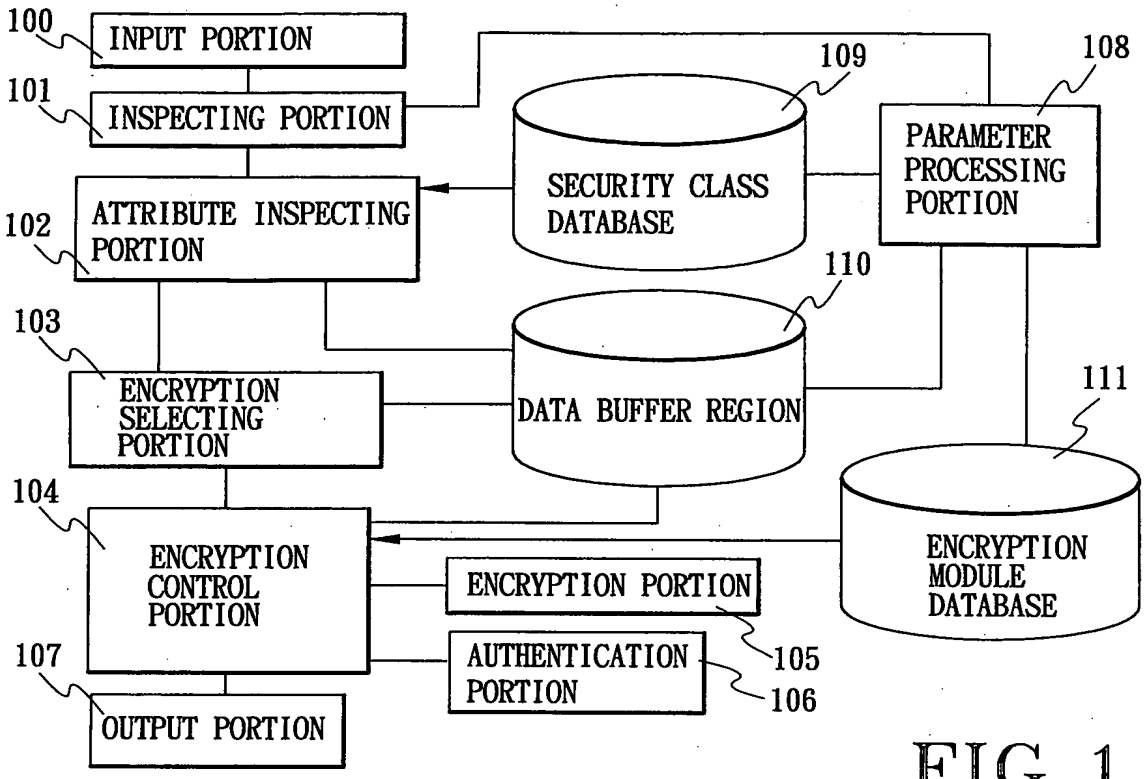
100
INPUT PORTION
101
INSPECTING PORTION
102
ATTRIBUTE INSPECTING PORTION
103
ENCRYPTION SELECTING PORTION
104
ENCRYPTION CONTROL PORTION
107
OUTPUT PORTION
109
SECURITY CLASS DATABASE
108
PARAMETER PROCESSING PORTION
110
DATA BUFFER REGION
111
ENCRYPTION MODULE DATABASE
ENCRYPTION PORTION
105
AUTHENTICATION PORTION
106

FIG. 1

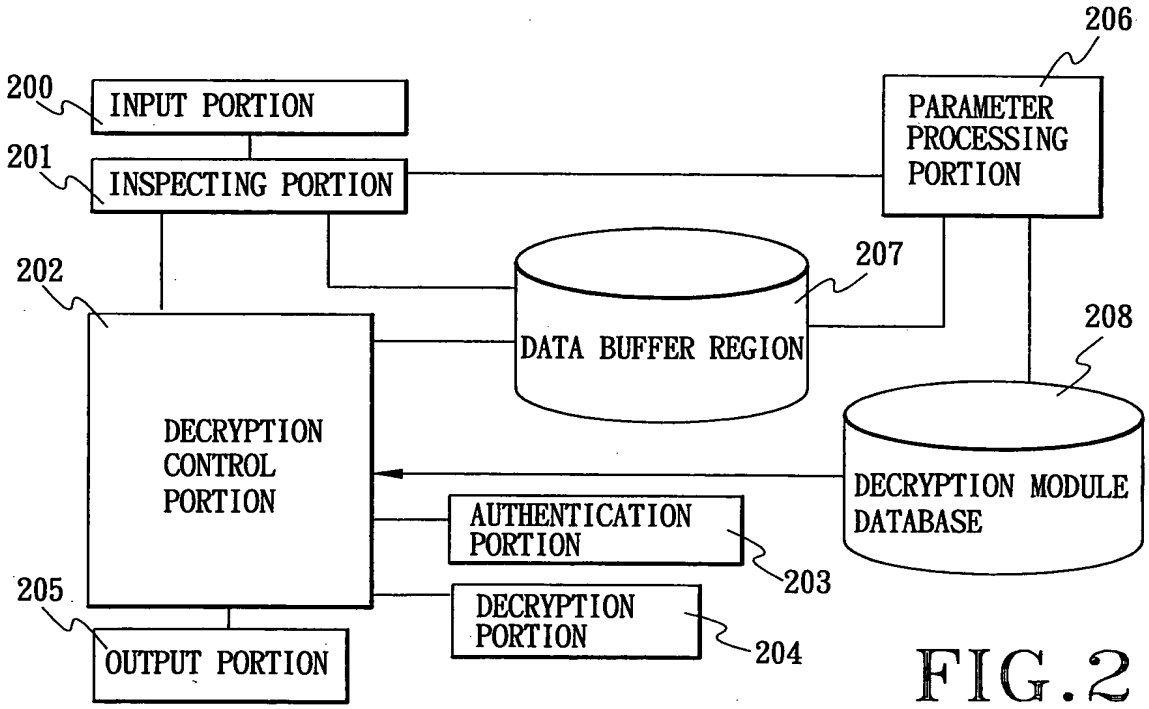
200
INPUT PORTION
201
INSPECTING PORTION
202
DECRYPTION CONTROL PORTION
205
OUTPUT PORTION
206
PARAMETER PROCESSING PORTION
207
DATA BUFFER REGION
208
DECRYPTION MODULE DATABASE
AUTHENTICATION PORTION
203
DECRYPTION PORTION
204

FIG. 2

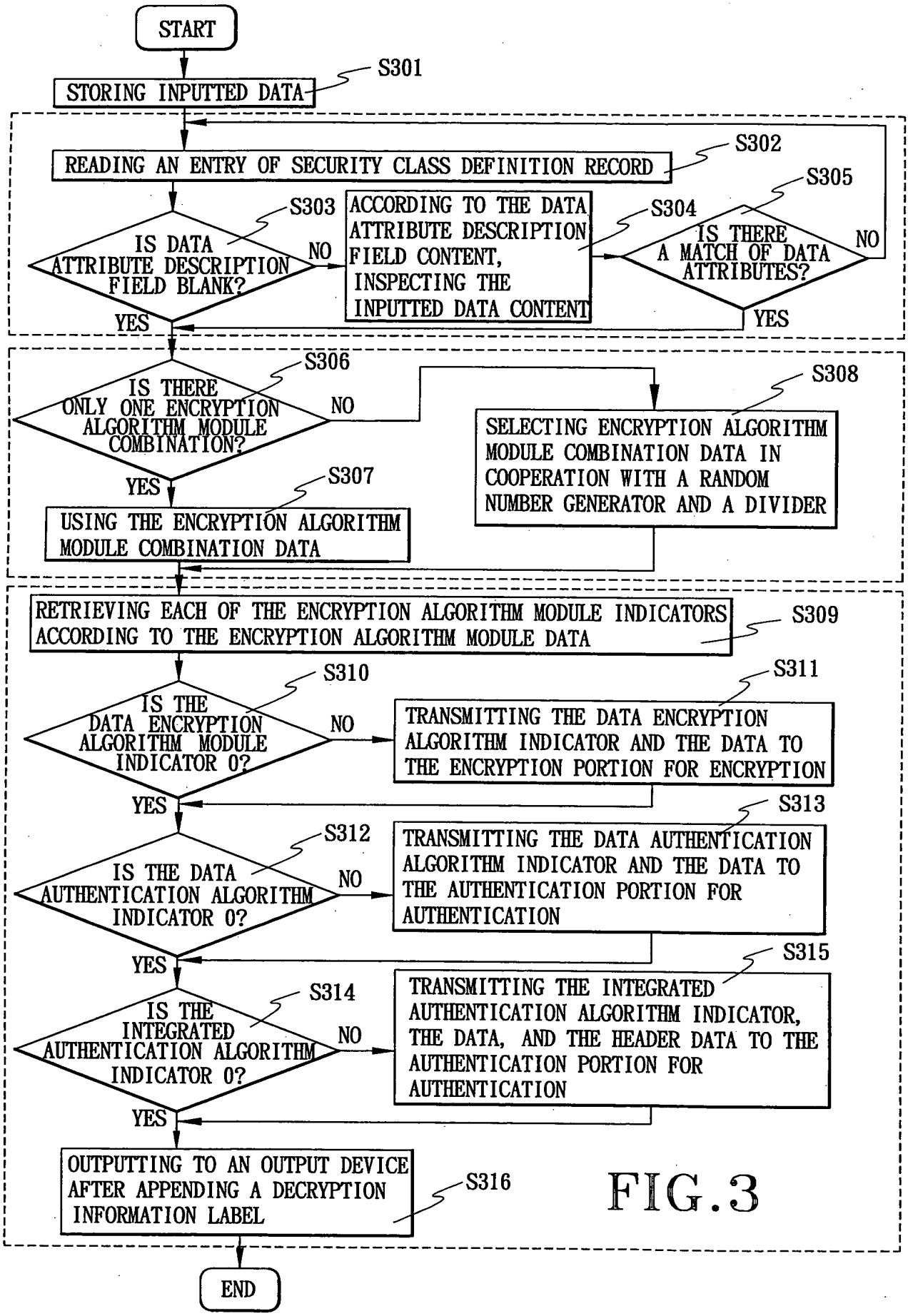
START
STORING INPUTTED DATA
S301
READING AN ENTRY OF SECURITY CLASS DEFINITION RECORD
S302
IS DATA ATTRIBUTE DESCRIPTION FIELD BLANK?
S303
NO
YES
ACCORDING TO THE DATA ATTRIBUTE DESCRIPTION FIELD CONTENT, INSPECTING THE INPUTTED DATA CONTENT
S304
IS THERE A MATCH OF DATA ATTRIBUTES?
S305
NO
YES
IS THERE ONLY ONE ENCRYPTION ALGORITHM MODULE COMBINATION?
S306
NO
YES
USING THE ENCRYPTION ALGORITHM MODULE COMBINATION DATA
S307
SELECTING ENCRYPTION ALGORITHM MODULE COMBINATION DATA IN COOPERATION WITH A RANDOM NUMBER GENERATOR AND A DIVIDER
S308
RETRIEVING EACH OF THE ENCRYPTION ALGORITHM MODULE INDICATORS ACCORDING TO THE ENCRYPTION ALGORITHM MODULE DATA
S309
IS THE DATA ENCRYPTION ALGORITHM MODULE INDICATOR 0?
S310
NO
YES
TRANSMITTING THE DATA ENCRYPTION ALGORITHM INDICATOR AND THE DATA TO THE ENCRYPTION PORTION FOR ENCRYPTION
S311
IS THE DATA AUTHENTICATION ALGORITHM INDICATOR 0?
S312
NO
YES
TRANSMITTING THE DATA AUTHENTICATION ALGORITHM INDICATOR AND THE DATA TO THE AUTHENTICATION PORTION FOR AUTHENTICATION
S313
IS THE INTEGRATED AUTHENTICATION ALGORITHM INDICATOR 0?
S314
NO
YES
TRANSMITTING THE INTEGRATED AUTHENTICATION ALGORITHM INDICATOR, THE DATA, AND THE HEADER DATA TO THE AUTHENTICATION PORTION FOR AUTHENTICATION
S315
OUTPUTTING TO AN OUTPUT DEVICE AFTER APPENDING A DECRYPTION INFORMATION LABEL
S316
END

FIG.3

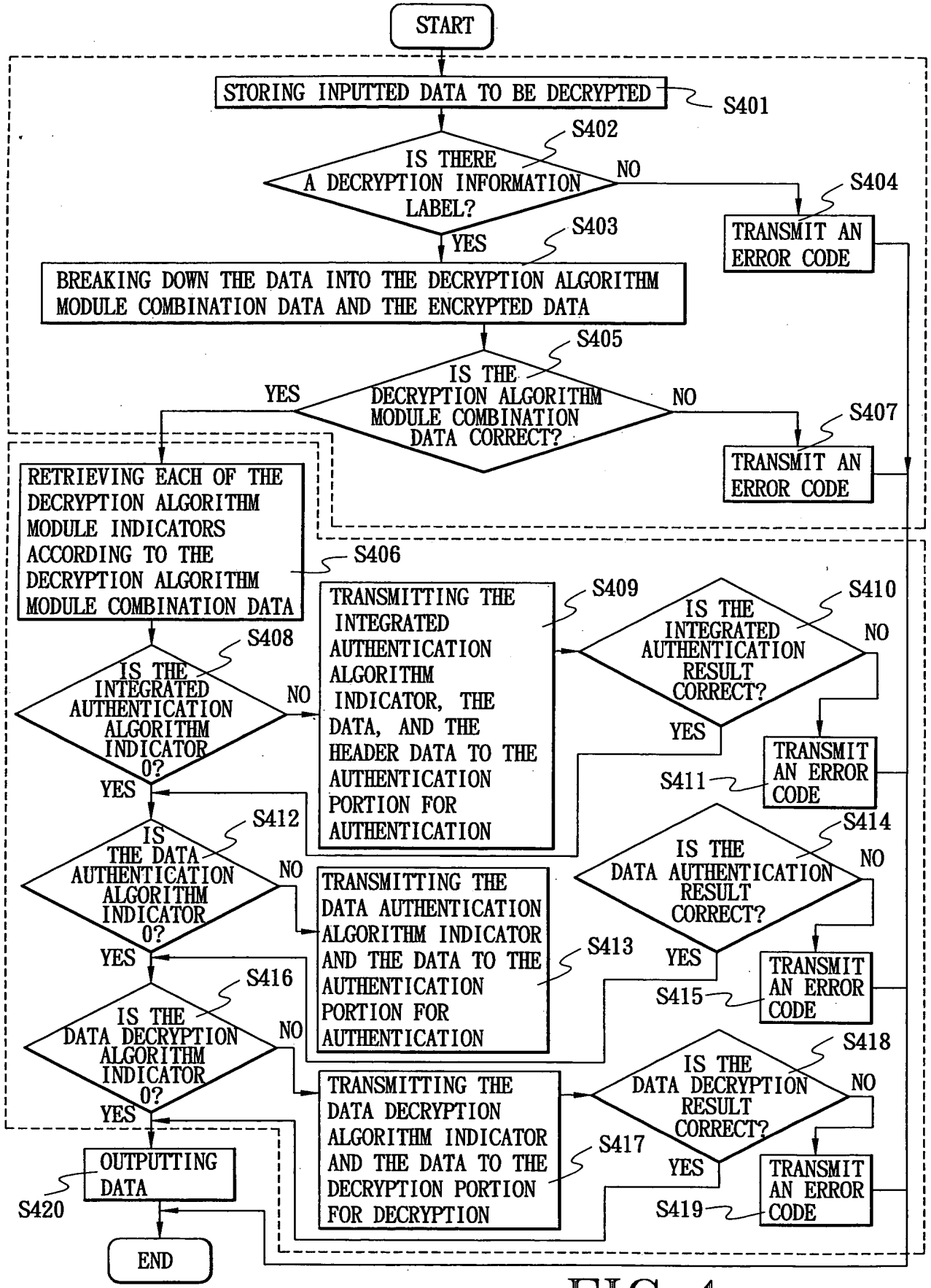
START
STORING INPUTTED DATA TO BE DECRYPTED
S401
S402
IS THERE A DECRYPTION INFORMATION LABEL?
NO
S404
TRANSMIT AN ERROR CODE
YES
S403
BREAKING DOWN THE DATA INTO THE DECRYPTION ALGORITHM MODULE COMBINATION DATA AND THE ENCRYPTED DATA
S405
IS THE DECRYPTION ALGORITHM MODULE COMBINATION DATA CORRECT?
YES
NO
S407
TRANSMIT AN ERROR CODE
RETRIEVING EACH OF THE DECRYPTION ALGORITHM MODULE INDICATORS ACCORDING TO THE DECRYPTION ALGORITHM MODULE COMBINATION DATA
S406
S408
IS THE INTEGRATED AUTHENTICATION ALGORITHM INDICATOR 0?
NO
YES
TRANSMITTING THE INTEGRATED AUTHENTICATION ALGORITHM INDICATOR, THE DATA, AND THE HEADER DATA TO THE AUTHENTICATION PORTION FOR AUTHENTICATION
S409
S410
IS THE INTEGRATED AUTHENTICATION RESULT CORRECT?
NO
YES
S411
TRANSMIT AN ERROR CODE
S412
IS THE DATA AUTHENTICATION ALGORITHM INDICATOR 0?
NO
YES
TRANSMITTING THE DATA AUTHENTICATION ALGORITHM INDICATOR AND THE DATA TO THE AUTHENTICATION PORTION FOR AUTHENTICATION
S413
S414
IS THE DATA AUTHENTICATION RESULT CORRECT?
NO
YES
S415
TRANSMIT AN ERROR CODE
S416
IS THE DATA DECRYPTION ALGORITHM INDICATOR 0?
NO
YES
TRANSMITTING THE DATA DECRYPTION ALGORITHM INDICATOR AND THE DATA TO THE DECRYPTION PORTION FOR DECRYPTION
S417
S418
IS THE DATA DECRYPTION RESULT CORRECT?
NO
YES
S419
TRANSMIT AN ERROR CODE
OUTPUTTING DATA
S420
END

FIG.4

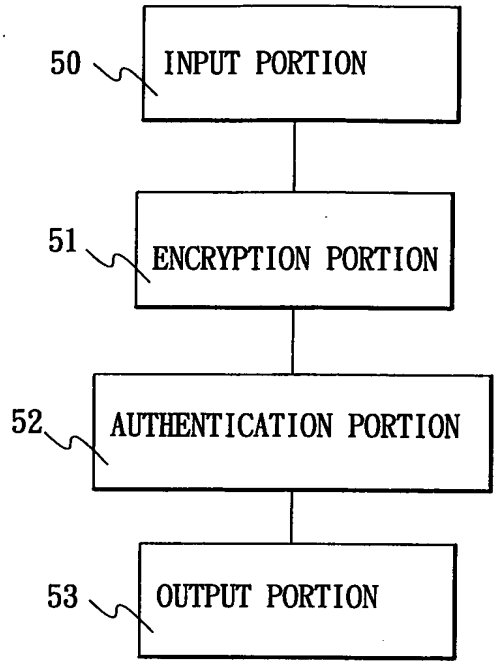
50
INPUT PORTION
51
ENCRYPTION PORTION
52
AUTHENTICATION PORTION
53
OUTPUT PORTION

FIG.5

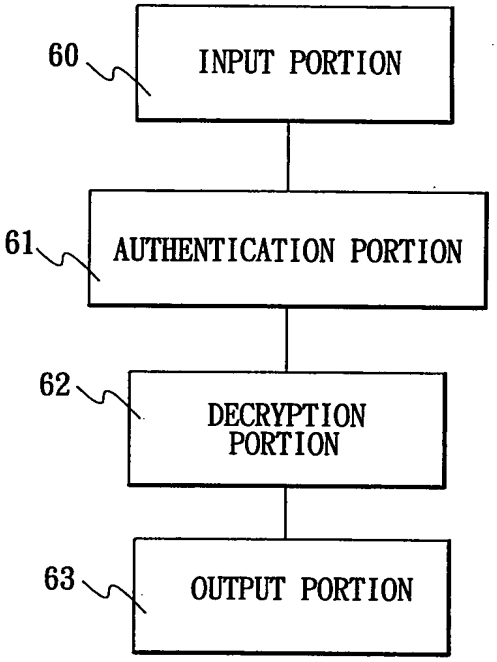
60
INPUT PORTION
61
AUTHENTICATION PORTION
62
DECRYPTION PORTION
63
OUTPUT PORTION

FIG.6

DATA ATTRIBUTE DESCRIPTION FIELD (24 BYTES)	ENCRYPTION DEFINITION FIELD (8 BYTES)
DATA ATTRIBUTE DESCRIPTION 1	ENCRYPTION DEFINITION 1
DATA ATTRIBUTE DESCRIPTION 2	ENCRYPTION DEFINITION 2
DATA ATTRIBUTE DESCRIPTION 3	ENCRYPTION DEFINITION 3
DATA ATTRIBUTE DESCRIPTION N	ENCRYPTION DEFINITION N

FIG.7

DATA ATTRIBUTE DESCRIPTION COMMAND	DESCRIPTION
00	BLANK DATA ATTRIBUTE DESCRIPTION VALUE, REPRESENTING PREDETERMINED SECURITY CLASS DEFINIFION
	RECORD LOGIC OPERATOR
01 EXPR1 EXPR2	AND OPERATOR EXPR1 AND EXPR2
02 EXPR1 EXPR2	OR OPERATOR EXPR1 OR EXPR2
03 EXPR1	NOT OPERATOR NOT EXPR2
	CONDITION EXPRESSION
04 AA BBBBBBBB	SOURCE ADDRESS IP IS IDENTICAL WITH THE FIRST AA BYTES OF
	BBBBBBBB
05 AA BBBBBBBB	DESTINATION ADDRESS IP IS IDENTICAL WITH THE FIRST AA BYTES OF BBBBBBBB
06 AA	COMMUNICATIONS PROTOCOL VALUE IS AA
07 AAAA BB	DATA AT ADDRESS AAAA, THE ONE-BYTE VALUE THEREOF BEING IDENTICAL WITH BB
08 AAAA BBBB	DATA AT ADDRESS AAAA, THE TWO-BYTE VALUE THEREOF BEING IDENTICAL WITH BBBB
09 AAAA BBBBBBBB	DATA AT ADDRESS AAAA, THE FOUR-BYTE VALUE BEING IDENTICAL WITH BBBBBBBB
0A~FE	RESERVED VALUE
FF	INDICATE THE ENDING VALUE IN DATA ATTRIBUTE DESCRIPTION FIELD

FIG.8

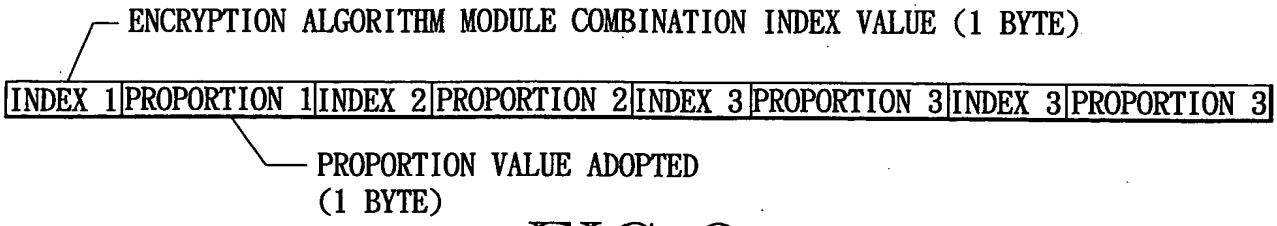

FIG.9

INDEX	DATA ENCRYPTION ALGORITHM INDICATOR FIELD(4-BYTE)	DATA AUTHENTICATION ALGORITHM INDICATOR FIELD(4-BYTE)	INTEGRATED AUTHENTICATION ALGORITHM INDICATOR FIELD(4-BYTE)
1	DATA ENCRYPTION ALGORITHM INDICATOR 1	DATA AUTHENTICATION ALGORITHM INDICATOR 1	INTEGRATED AUTHENTICATION ALGORITHM INDICATOR 1
2	DATA ENCRYPTION ALGORTTHM INDICATOR 2	DATA AUTHENTICATION ALGORITHM INDICATOR 2	INTEGRATED AUTHENTICATION ALGORITHM INDICATOR 2
3	DATA ENCRYPTION ALGORTTHM INDICATOR 3	DATA AUTHENTICATION ALGORITHM INDICATOR 3	INTEGRATED AUTHENTICATION ALGORITHM INDICATOR 3
N	DATA ENCRYPTION ALGORTTHM INDICATOR N	DATA AUTHENTICATION ALGORITHM INDICATOR N	INTEGRATED AUTHENTICATION ALGORITHM INDICATOR N

FIG.10

INDEX	DATA DECRYPTION ALGORITHM INDICATOR FIELD(4-BYTE)	DATA AUTHENTICATION ALGORITHM INDICATOR FIELD(4-BYTE)	INTEGRATED AUTHENTICATION ALGORITHM INDICATOR FIELD(4-BYTE)
1	DATA DECRYPTION ALGORITHM INDICATOR 1	DATA AUTHENTICATION ALGORITHM INDICATOR 1	INTEGRATED AUTHENTICATION ALGORITHM INDICATOR 1
2	DATA DECRYPTION ALGORITHM INDICATOR 2	DATA AUTHENTICATION ALGORITHM INDICATOR 2	INTEGRATED AUTHENTICATION ALGORITHM INDICATOR 2
3	DATA DECRYPTION ALGORITHM INDICATOR 3	DATA AUTHENTICATION ALGORITHM INDICATOR 3	INTEGRATED AUTHENTICATION ALGORITHM INDICATOR 3
N	DATA DECRYPTION ALGORITHM INDICATOR N	DATA AUTHENTICATION ALGORITHM INDICATOR N	INTEGRATED AUTHENTICATION ALGORITHM INDICATOR N

FIG.11

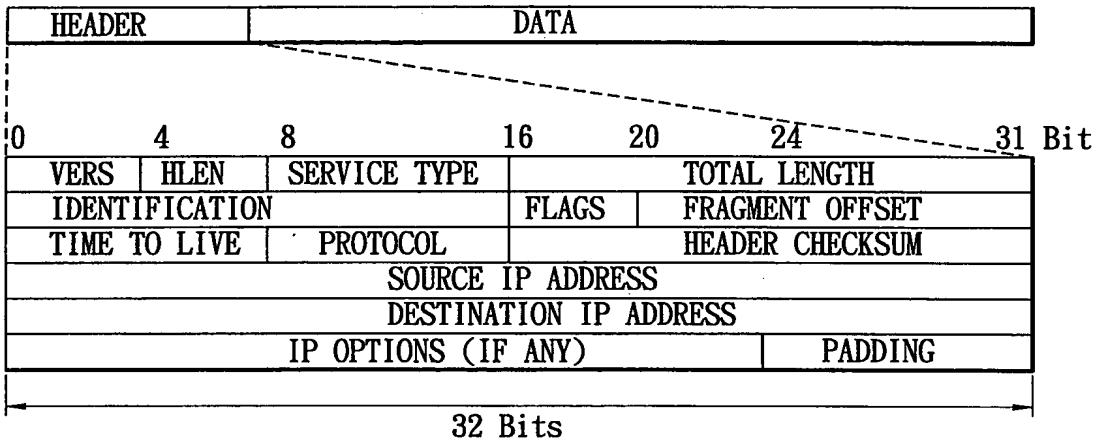
HEADER
DATA
0
4
8
16
20
24
31 Bit
VERS
HLEN
SERVICE TYPE
TOTAL LENGTH
IDENTIFICATION
FLAGS
FRAGMENT OFFSET
TIME TO LIVE
PROTOCOL
HEADER CHECKSUM
SOURCE IP ADDRESS
DESTINATION IP ADDRESS
IP OPTIONS (IF ANY)
PADDING
32 Bits

FIG. 12

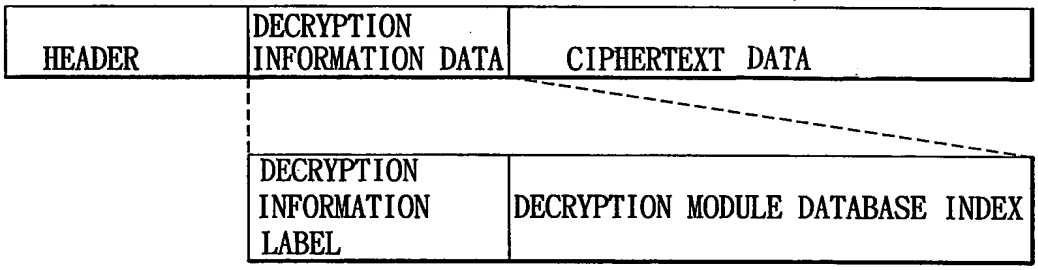
HEADER
DECRYPTION INFORMATION DATA
CIPHERTEXT DATA
DECRYPTION INFORMATION LABEL
DECRYPTION MODULE DATABASE INDEX

FIG. 13

14a

HEADER	DATA

0	4	8	16	20	24	31 Bit
VERS	HLEN	SERVICE TYPE	TOTAL LENGTH			
IDENTIFICATION			FLAGS	FRAGMENT OFFSET		
TIME TO LIVE		PROTOCOL	HEADER CHECKSUM			
SOURCE IP ADDRESS=0xC0A80001						
DESTINATION IP ADDRESS=0xAC100001						
IP OPTIONS (IF ANY)					PADDING	

32 Bits

14b

DATA ATTRIBUTE DESCRIPTION FIELD	ENCRYPTION DEFINITION FIELD
01 04 18 C0A80000 05 18 AC100000 FF...	01 03 02 03 03 01 04 01
02 09 0034 55534552 09 0034 50415353 FF..	03 01 FF...
07 00 09 50 FF...	04 01 FF...
01 07 00 09 51 07 00 14 50 FF...	05 01 FF...
00 FF...	01 05 02 04 04 01 FF...

14c

INDEX	DATA ENCRYPTION ALGORITHM INDICATOR FIELD	DATA AUTHENTICATION ALGORITHM INDICATOR FIELD	INTEGRATED AUTHENTICATION ALGORITHM INDICATOR FIELD
1	DES ENCRYPTION ALGORITHM INDICATOR	MD5 AUTHENTICATION ALGORITHM INDICATOR	0
2	DES ENCRYPTION ALGORITHM INDICATOR	SHA1 AUTHENTICATION ALGORITHM INDICATOR	MD5 AUTHENTICATION ALGORITHM INDICATOR
3	3DES ENCRYPTION ALGORITHM INDICATOR	SHA1 AUTHENTICATION ALGORITHM INDICATOR	SHA1 AUTHENTICATION ALGORITHM INDICATOR
4	0	0	SHA1 AUTHENTICATION ALGORITHM INDICATOR
5	0	0	0

14b

HEADER	DECRYPTION INFORMATION DATA	CIPHERTEXT DATA

DECRYPTION INFORMATION LABEL	DECRYPTION MODULE DATABASE INDEX=2

FIG. 14

15a

HEADER	DECRYPTION INFORMATION DATA	CIPHERTEXT DATA

DECRYPTION INFORMATION LABEL	DECRYPTION MODULE DATABASE INDEX=2

15b

INDEX	DATA DECRYPTION ALGORITHM INDICATOR FIELD	DATA AUTHENTICATION ALGORITHM INDICATOR FIELD	INTEGRATED AUTHENTICATION ALGORITHM INDICATOR FIELD
1	DES DECRYPTION ALGORITHM INDICATOR	MD5 AUTHENTICATION ALGORITHM INDICATOR	0
2	DES DECRYPTION ALGORITHM INDICATOR	SHA1 AUTHENTICATION ALGORITHM INDICATOR	MD5 AUTHENTICATION ALGORITHM INDICATOR
3	DES DECRYPTION ALGORITHM INDICATOR	SHA1 AUTHENTICATION ALGORITHM INDICATOR	SHA1 AUTHENTICATION ALGORITHM INDICATOR
4	0	0	SHA1 AUTHENTICATION ALGORITHM INDICATOR
5	0	0	0

15c

HEADER	PLAINTEXT DATA

FIG. 15

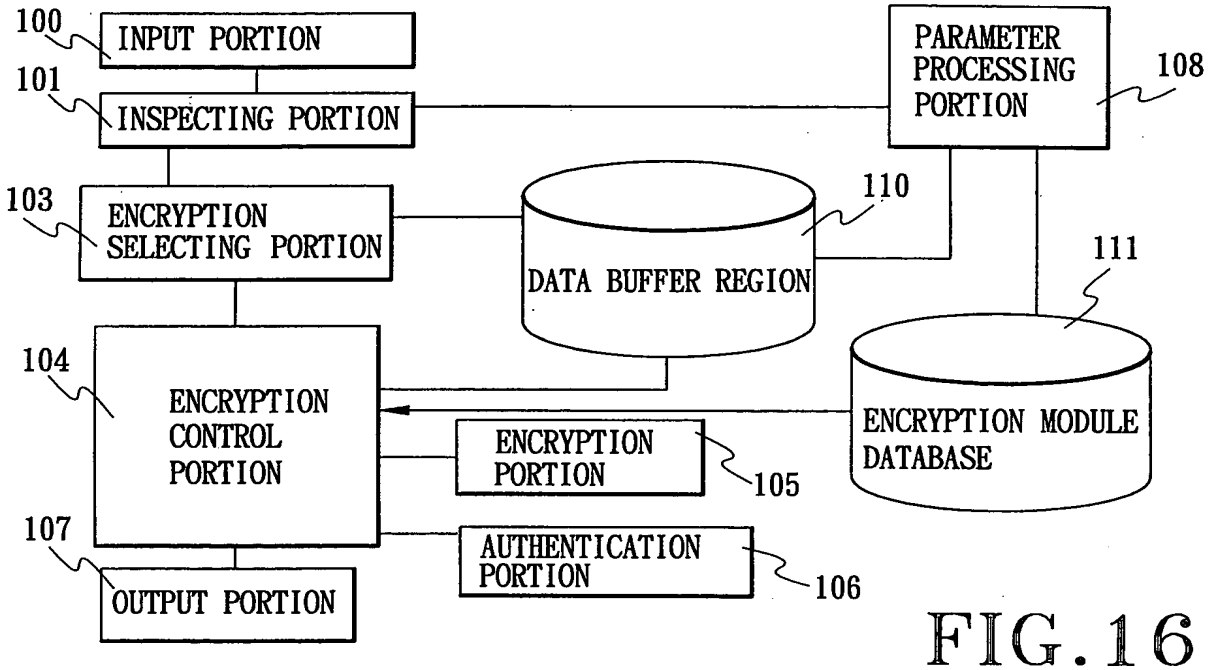
100
INPUT PORTION
101
INSPECTING PORTION
103
ENCRYPTION SELECTING PORTION
104
ENCRYPTION CONTROL PORTION
107
OUTPUT PORTION
PARAMETER PROCESSING PORTION
108
110
DATA BUFFER REGION
111
ENCRYPTION MODULE DATABASE
ENCRYPTION PORTION
105
AUTHENTICATION PORTION
106

FIG. 16

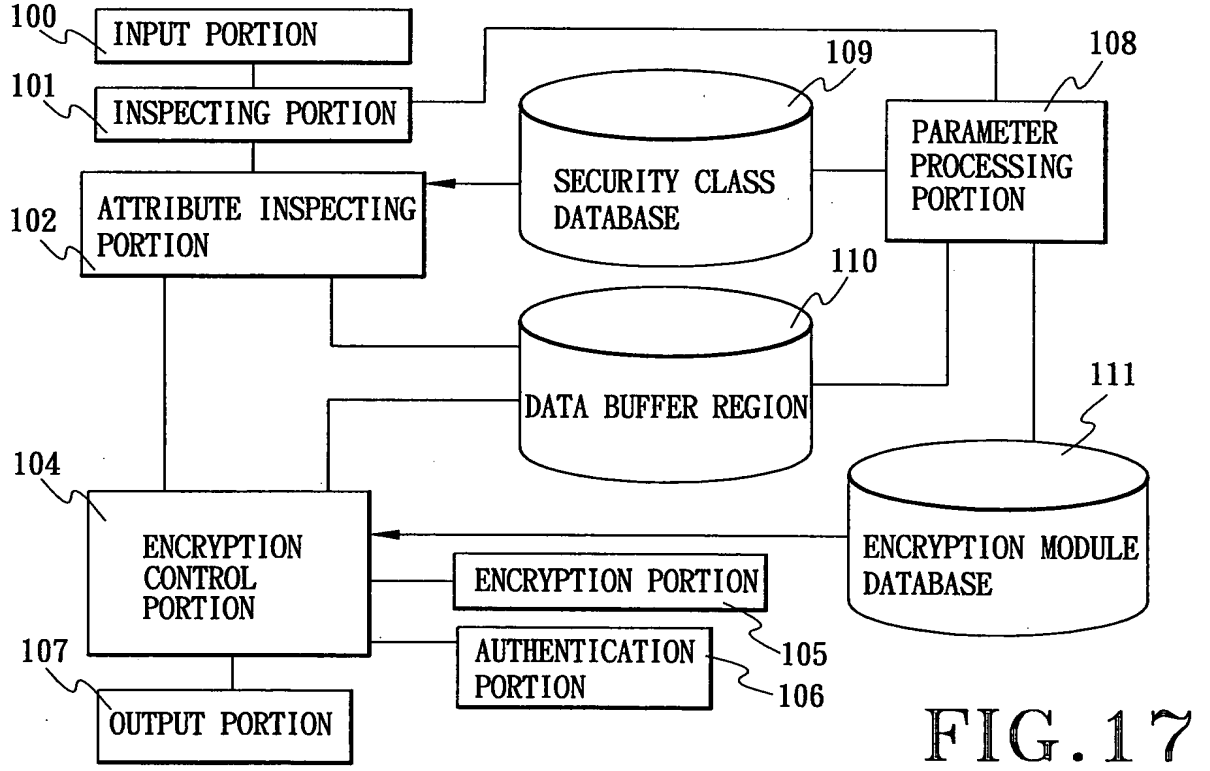
100
INPUT PORTION
101
INSPECTING PORTION
102
ATTRIBUTE INSPECTING PORTION
104
ENCRYPTION CONTROL PORTION
107
OUTPUT PORTION
109
SECURITY CLASS DATABASE
108
PARAMETER PROCESSING PORTION
110
DATA BUFFER REGION
111
ENCRYPTION MODULE DATABASE
ENCRYPTION PORTION
105
AUTHENTICATION PORTION
106

FIG. 17